# CLAIMS

What is claimed is:

1. A secure message generation system comprising:

a service pair encryption component that employs an initiator private key to encrypt authentication information;

a key exchange key encryption component that employs a target public key to encrypt a key exchange key;

a dialog session key encryption component that employs the key exchange key to encrypt a dialog session key;

a message body encryption component that employs the dialog session key to encrypt a message body; and,

a message generator that provides an encrypted message based, at least in part, upon the encrypted authentication information, the encrypted key exchange key, the encrypted dialog session key and the encrypted message body.

2. The system of claim 1, the message generator generates a security preamble of the encrypted message.

3. The system of claim 2, the security preamble comprising at least one of a version information field, a message integrity check information field, a time associated with creation of the message field and an encryption salt value used for the message field.

4. The system of claim 1, the service pair encryption component generates a service pair security header of the encrypted message based, at least in part, upon the initiator private key.

5. The system of claim 4, the service pair security header comprising at least one of an initiator certificate name field, an initiator certificate issue date field, a target certificate name field, a target certificate name field and a signature field.

6. The system of claim 5, the signature field comprising a one-way hash of the initiator certificate name field, the initiator certificate issue date field, the target certificate name field and the target certificate name field encrypted with the initiator private key.

7. The system of claim 1, the key exchange key encryption component generates a key exchange key header of the encrypted message based, at least in part, upon the target public key.

8. The system of claim 7, the key exchange key header comprising a key exchange key identifier and an encrypted key exchange key.

9. The system of claim 7, the key exchange key comprising a symmetric key.

10. The system of claim 9, the key exchange key comprising a 128-bit symmetric key.

11. The system of claim 1, the key exchange key uniquely assigned to an initiator and a target pair.

12. The system of claim 11, messages exchanged between the initiator and target pair being based, at least in part, upon the unique key exchange key.

13. The system of claim 1, the dialog session key encryption component generates a dialog session key header of the encrypted message based, at least in part, upon the key exchange key.

14. The system of claim 13, the dialog session key header comprising a dialog session key identifier field and an encrypted dialog session key field.

15. The system of claim 1, the message body encryption component computes a message integrity check on message and header data.

16. The system of claim 15, the message integrity check is computed using a one-way hash algorithm.

17. A secure message receiver system comprising:

a message receiver that receives an encrypted message;

a service pair encryption component that employs an initiator public key to decrypt authentication information of the encrypted message;

a key exchange key decryption component that employs a target private key to decrypt a key exchange key of the encrypted message, if the key exchange key is not stored in a cache;

a dialog session key decryption component that employs the key exchange key to decrypt a dialog session key of the encrypted message, if the dialog session key is not stored in the cache; and,

a message body decryption component that employs the dialog session key to decrypt a message body of the encrypted message.

18. The system of claim 17 further comprising the message receiver determines whether information associated with the key exchange key and/or the dialog session key have been cached based, at least in part, upon an endpoint state associated with a dialog.

19. The system of claim 17, the encrypted message comprising a service pair security header, a key exchange key header, a dialog session key header and a message body.

20. The system of claim 19, the service pair security header comprising at least one of an initiator certificate name field, an initiator certificate issue date field, a target certificate name field, a target certificate name field and a signature field.

21. The system of claim 19, the key exchange key header comprising a key exchange key identifier and an encrypted key exchange key.

22. The system of claim 19, the dialog session key header comprising a dialog session key identifier field and an encrypted dialog session key field.

23. The system of claim 17, the encrypted message further comprising a security preamble, the security preamble comprising at least one of a version information field, a message integrity check information field, a time associated with creation of the message field and an encryption salt value used for the message field.

24. The system of claim 17, the key exchange key uniquely assigned to an initiator and a target pair.

25. The system of claim 24, messages exchanged between the initiator and target pair being based, at least in part, upon the unique key exchange key.

26. A method facilitating secure message generation comprising:

providing encrypted authentication information, the encryption being based, at least in part, upon an initiator private key;

providing an encrypted key exchange key, the encryption being based, at least in part, upon a target public key;

providing an encrypted dialog session key, the encryption being based, at least in part, upon the key exchange key; and,

providing an encrypted message body, encryption being based, at least in part, upon the dialog session key.

27. The method of claim 26 further comprising:

providing an encrypted message based, at least in part, upon the encrypted authentication information, the encrypted key exchange key, the encrypted dialog session key and the encrypted message body.

28. The method of claim 26, a service pair security header comprising the encrypted authentication information, a key exchange key header comprising the encrypted key exchange key, and, a dialog session key header comprising the encrypted dialog session key.

29. The method of claim 28, further comprising at least one of the following:

employing the initiator private key to encrypt authentication information, if the service pair security header is not cached;

employing the target public key to encrypt the key exchange key, if the key exchange key header is not cached; and,

employing the key exchange key to encrypt the dialog session key, if the dialog session key header it not cached.

30. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 26.

31. A method of receiving a secure message comprising:

receiving an encrypted message; and,

decrypting the encrypted message with a dialog session key, if a service pair security header, a key exchange key header and a dialog session key header associated with the encrypted message have been stored.

32. The method of claim 31, the service pair security header comprising encrypted authentication information, the key exchange key header comprising an encrypted key exchange key, and, the dialog session key header comprising an encrypted dialog session key.

33. The method of claim 32, further comprising at least one of the following:

decrypting authentication information, if the service pair security header is not cached, decryption being based, at least in part, upon an initiator public key;

decrypting the key exchange key, if the key exchange key header is not cached, decryption being based, at least in part, upon a target private key; and,

decrypting the dialog session key, if the dialog session key header is not cached, decryption being based, at least in part, upon the key exchange key.

34. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 31.

35. A data packet transmitted between two or more computer components that facilitates secure communication, the data packet comprising:

a key exchange key header comprising an encrypted key exchange key;

a dialog session key header comprising a dialog session key encrypted with the key exchange key; and,

a message body field comprising a message encrypted with the dialog session key.